Microsoft®

Windows NT® Server

Server Operating System

Planning for a Global Directory Service

White Paper

© 1998 Microsoft Corporation. All rights reserved.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft, the BackOffice logo, BackOffice, JScript,Outlook, NetShow, Visual Basic and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product or company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0398

CONTENTS

OVERVIEW....1

THE NEED FOR GLOBAL DIRECTORY SERVICES....2

GLOBAL DIRECTORY SERVICE REQUIREMENTS....3

MICROSOFT'S GLOBAL DIRECTORY SERVICE STRATEGY....4
Microsoft's Windows NT Server 4.0 Directory Interoperability Offerings 4
Windows NT Server 4.0 Public Protocols and Interfaces 5
Third-Party Offerings for Windows NT Server 4.0 Directory Interoperability 6
Active Directory and Windows NT Server 5.0 7
Active Directory's Support for Standards 9
Active Directory Interoperability, Synchronization and Migration 10

CONCLUSION....12

OVERVIEW

Today, information about people, applications, and resources is scattered throughout most IT enterprises – and is continuing to proliferate. For reasons of enhanced functionality, operating systems and applications (ranging from e-mail to ERP systems) frequently provide their own repositories to store information about users and resources. As companies continually increase the number of applications and platforms that they use and support, the number of different repositories increases as well. This forces companies to manage information in many different places – even when those places contain duplicated and related information. To minimize costs and increase their ability to respond to change, companies need an enterprise-class *directory service* that provides common place to store, access and manage corporate information *and* that doesn't sacrifice application and operating system functionality.

Because of the lifecycle realities of important existing investments in applications and platforms, this goal cannot be achieved overnight. However, with available, internet-ready directory standards, and the growing response from application vendors to customers' demands for interoperability, it is possible for companies to reduce the number of directories that they need, and lay the groundwork for moving to a global directory strategy in the future.

The focal point of Microsoft's directory service strategy is the Microsoft Windows NT Server 5.0 Active Directory (Active Directory). Active Directory is the first enterprise-class directory service that is scalable, built from the ground up using Internet-standard technologies, and is fully integrated with the operating system. In addition to providing comprehensive directory services to Windows applications, Active Directory is designed to be a consolidation point for isolating, migrating, centrally managing and reducing the number of directories that companies have. This makes Active Directory the ideal long-term foundation for corporate information sharing and common management of network resources including applications, network operating systems, and directory-enabled devices.

Microsoft realizes that companies have significant investments in existing applications and operating systems (including Window NT Server 4.0) and that it will take time to fully exploit the benefits of Active Directory. Therefore, Microsoft has:

- Developed open directory service interfaces that developers can use today when building and deploying applications for Windows NT Server 4.0
- Built tools that upgrade companies from Windows NT Server 4.0 to Active Directory, preserving all directory-related information intact
- Provided synchronization features in Active Directory that let

companies begin to us Active Directory immediately as their focal point for centralized management and single sign-on infrastructures while transitioning away from existing directories

- Created automated ways to migrate to Active Directory from other directories

For companies that use Windows NT Server 4.0 today, and for companies that plan to use Windows NT Server 5.0 in the future, Active Directory is the smart choice for a global directory strategy.

In simple terms, directory services are repositories for information about network-based entities such as applications, files, printers, and people. Directory services are important because they provide a consistent way to name, describe, locate, access, manage, and secure information about these resources.

Many vendors build specialized repositories or directory services into their operating systems and applications to enable the specific functionality their customers require. For example, e-mail products include directory services that enable users to look up and send mail to others, and server operating systems use directory services for features such as user account management and to store configuration information about applications. Because these directory services are targeted narrowly at the needs of the application or operating system, and often lack standards-based interfaces, most companies have found that they are responsible for many different directories that cannot be managed centrally or interoperate easily with each other.

Having many, incompatible directory services means that:

- **End users** must use multiple user accounts and passwords to log in to different systems and they must know the exact locations of information on the network.
- **Administrators** must understand how to manage each directory within the network and must duplicate many steps when procedures, such as adding a new employee to a company, involve many different directories.
- **Application developers** must write different logic for every directory that their applications need to access.

As a result, the proliferation of customized directory services translates directly to companies as a continually rising cost of ownership in the form of management, lost end-user productivity, and application complexity. In the near term, companies need to find ways to halt this trend and minimize the total number of directories that they have through proactive consolidation. Over the longer term, the best solution is to standardize on technologies that provide the required levels of

GLOBAL DIRECTORY SERVICE REQUIREMENTS

scalability, standards-based interoperability, and operating system integration.

There are a number of key requirements that global directory services must satisfy in order to be effective in complex corporate environments:

- **Single sign-on:** End users want the ability to log on once using a single user name and password and gain access to their e-mail, applications, files and network resources such as printers regardless of their location on the network.
- **Centralized management:** Administrators want the ability to manage all corporate resources centrally. They should not have to repeat the same steps in multiple directories to conduct common management tasks such as adding or deleting user accounts.
- **Flexibility to support change:** Business managers need a directory service that enables their companies to respond quickly to change. For example, directory services should facilitate – not hinder – reorganization within their company, and simplify – not complicate – the implementation of corporate mergers. In addition, managers need directory services that enable them to use the Internet to work with partners and to support electronic commerce in a dynamic business environment.
- **Standards-based interfaces:** Application developers need directory services that provide a comprehensive set of features *and* support common standards and programming interfaces. The directory service must also be tightly integrated with the operating system so that developers don't need to duplicate functionality such as security infrastructures within their application.

To address these requirements, customers ultimately need to identify a scalable, powerful, flexible and standards-based directory service that is capable of supporting consolidation efforts today and can function successfully as a global directory service in the future. Therefore, the ideal long-term global directory strategy will be based on technologies that:

- Are built from the ground up using Internet standards
- Provide published interfaces for directory access, interoperability, migration, and synchronization with other transitional directories
- Are integrated at the operating system level for simplicity, enhanced functionality and system integrity

A directory service that meets these requirements is a smart long-term investment because it ensures that companies will be investing in path to

a single, general-purpose directory service that integrates with the multiple, special-purpose directories that companies have today.

The focal point of Microsoft's directory service strategy is the Microsoft Windows NT Server 5.0 Active Directory (Active Directory). Active Directory is the first enterprise-class directory service that is scalable, built from the ground up using Internet-standard technologies, and is fully integrated at the operating system level. In addition to providing comprehensive directory services to Windows applications, Active Directory is designed to be a consolidation point for isolating, migrating, centrally managing and reducing the number of directories that companies have. This makes Active Directory the ideal long-term foundation for corporate information sharing and common management of network resources including applications, network operating systems, and directory-enabled devices.

Microsoft recognizes that the success of Active Directory is based on many factors. Microsoft treats some, such as scalability and performance, as fundamental technical requirements that are easy to define. Other factors, such as protecting existing investments, are harder to define in absolute terms. For these factors, Microsoft has identified a set of guiding principles:

- Existing and future users of Windows NT 4.0 must have a wide-range of options available for interoperating with existing directories and applications. These options should come from Microsoft and from third parties.
- The migration from Windows NT Server 4.0 to Windows NT Server 5.0 and Active Directory must be seamless and cause no loss of existing directory-related data from the Windows NT 4.0 environment.
- Active Directory must be tightly integrated at the operating system level to ensure seamless operation, simplified management, enhanced functionality and system integrity.
- Active Directory must support as many standards-based interfaces as possible to facilitate longer-term consolidation around Active Directory as a single, global directory service.

The following sections describe these principles, and Microsoft's results, in more detail.

Microsoft's Windows NT Server 4.0 Directory Interoperability Offerings

Microsoft provides existing Windows NT Server 4.0 users with a number of facilities and features (that require no changes to existing systems) to

facilitate single sign-on by users and centralized management by administrators:

- **NetWare integration and migration:** Microsoft supplies NetWare customers with a number of tools designed to make it easy to integrate Windows NT Server into their existing NetWare–based networks. Among these are Services for NetWare, including tools for synchronizing Windows NT Server-based information with NetWare 2.x, 3.x and 4.x systems (in bindery emulation mode) seamlessly. These services also enable any NetWare client to use Windows NT Server for file and print sharing without having to change any client software. Windows NT Server also ships with a migration tool that allows customers to migrate NetWare user and group account information to the Windows NT directory services.
- **Macintosh integration:** Windows NT Services for the Macintosh, also included with Windows NT Server 4.0, provide AppleShare-compatible directory authentication and file and printer sharing using Apple's AppleTalk protocol.
- **Single sign-on for host systems:** SNA Server for Windows NT enables a single sign-on environment between Windows NT and host environments by providing synchronization with host-based RACF and ACF-2 security products.

Windows NT Server 4.0 Public Protocols and Interfaces

Microsoft recognizes that third-party interoperability products are critical to the success of Windows NT 4.0 and to the ultimate success of Windows NT 5.0 and Active Directory. To make it easier for third-parties to build solutions that will work well today and with Active Directory in the future, Microsoft provides several public interfaces and protocols:

- **Active Directory Service Interfaces (ADSI):** A set of high-level, language-independent directory service programming interfaces. ADSI includes support for working with resources provided by Windows NT Server 4.0, Novell NetWare 3.x, and NetWare 4.x including the Novell Directory Services (NDS). ADSI is also the primary API for developing to the Windows NT Server 5.0 Active Directory. ADSI provides developers with a standard, easy way to develop applications that can access information from multiple directories and implement applications that synchronize data between directories.
- **Light-Weight Directory Access Protocol (LDAP) Version 3:** An industry- standard directory access protocol. LDAP provides a standard way for desktop and server applications to access information from different directory implementations. Microsoft

provides LDAP support in client products (e.g., Microsoft Outlook™, NetMeeting™, Internet Explorer) and in server products (e.g., the current version of Site Server, Exchange Server). LDAP will also be the method used by Microsoft Exchange Server for directory migration and synchronization with Windows NT Server 5.0. And, Windows NT Server 5.0 will provide LDAP support for access to Active Directory-based information.

- **Security Service Provider Interface (SSPI)**: A set of high-level, language-independent programming interfaces for accessing Windows NT security features. SSPI, which is based on the General Security Service Application Programming Interface (GSSAPI) standard, enables developers to take advantage of the integrated security benefits of Windows NT including single sign-on, authentication and authorization.

In addition, one of the important requirements that third parties must meet to be part of the Microsoft BackOffice® Logo Program is to support Windows NT 4.0 single sign-on features. Currently, over 550 companies provide compliant products (some of which are listed below).

Third-Party Offerings for Windows NT Server 4.0 Directory Interoperability

In addition to the features provided in Microsoft products, the following third parties use the published interfaces described above to provide additional interoperability solutions for centralized administration, single sign-on, and domain configuration. These solutions do not require changes to existing systems that customers currently have in place, and facilitate the move to Active Directory in the future.

DirectScript from ~~Querisoft~~Entevo: An enterprise directory management product that eases administration and reduces total cost of ownership by simplifying common administration tasks. For example, DirectScript:

- Offers the simplicity of the Visual Basic® development system, Visual Basic Scripts (VBS) or J/Script™ development software to accomplish common administrative tasks such as moving resources between domains and managing security on file/print servers, or enumerating resources throughout the distributed network
- Uses Microsoft's ADSI, providing management of Users, Groups, Directory/Files, Security, Registry, Computer and Printer Objects in a Windows NT Domain environment
- Comes pre-packaged with over a dozen customizable samples and scripts (Visual Basic, Active Server Pages and J/Script). These management scripts can be used throughout the enterprise with the

help of a browser. The framework also allows for mapping disparate objects from different namespaces such as Novell's NDS.

SecureFile from ~~Querisoft~~Entevo: A desktop and Internet security tool designed to provide file security features to the personal and enterprise markets. For example, SecureFile provides users with file privacy (encryption/decryption), integrity (hashing), and authentication (sign/verify using digital signatures) services with an integrated point and click interface.

DirectAdmin from ~~Querisoft~~Entevo: A future release of DirectAdmin will have support for multiple network operating systems and applications (NDS, Vines, Exchange) along with support for inter-NOS operations for central management of these directories from Windows NT Server.

Enterprise Administration from Mission Critical: An advanced, rules-based administration environment for large-scale Windows NT-based networks providing administrative scalability through account and resource management, comprehensive reporting, and advanced automation capabilities including domain consolidation.

Virtual Administrator from FastLane Technologies: A tool that enables administrators to segment and delegate administrative rights within any Windows NT domain architecture and use standard Windows NT administration tools to flatten or reconfigure domains.

Enterprise Resource Manager from Axent: A product that enables users to log on to the network and automatically gain secure access to heterogeneous platforms without multiple logons. For example, Enterprise Resource Manager:

- Provides additional controls over user accounts, systems access rights, and passwords
- Allows system managers to partition administration activities securely and efficiently

Flyte Migration Management Tool for VINES to Windows NT: A tool that simplifies the task of migrating from VINES to Windows NT Server. Incorporating StreetTalk attributes and clean-up tools, Flyte delivers smooth, fast transition to Windows NT with minimum impact on users.

Phoenix Domain Reconfiguration Tool for Windows NT: A tool that simplifies domain reconfiguration and flattening. Transitions can be handled step-by-step or automatically, with security protection.

Active Directory and Windows NT Server 5.0

Active Directory is a fundamental component of the Windows NT Server

5.0 operating system platform. Active Directory addresses important long-term customer concerns because it:

- Is designed from the ground up using Internet standards for interoperability
- Provides published interfaces for directory interoperability, migration, and synchronization with other directory services
- Delivers tight integration of directory services with services in the operating system for system integrity, simplicity, enhanced functionality and extensibility

At first glance, the benefits of tight integration of directory services and an operating system may not be obvious. By ensuring that Active Directory is tightly integrated with Windows NT Server 5.0, however, Microsoft is able to offer significant benefits to companies and their users.

- **Enhanced system integrity:** By delivering Active Directory as part of Windows NT Server 5.0, Microsoft makes sure that the entire operating system platform has been optimized and tested for performance, security and reliability. As Windows NT Server is used increasingly in mission-critical roles, the ability to obtain a wide range of functionality from Microsoft directly is important.
- **Centralized management:** The Active Directory is where Windows NT Server 5.0 stores all information about system configuration, user profiles and applications. Combined with Windows NT Server 5.0 Policy Management features, administrators can manage distributed desktops, network services, and directory-enabled applications from a central location using a consistent management interface. Network administrators also have a consistent way to monitor and manage network devices, such as routers, through system profiles provided by the Active Directory.
- **Personalized user environments:** Features in Windows NT Server 5.0 and Windows NT Workstation 5.0 use information stored in Active Directory to determine the where a user stores their documents, where their personal settings are saved, and the general configuration of their environment. The configuration information is specified in the form of an administrative policy that is applied when a user logs in from a given machine. These policies determine the behavior of computing environment elements such as on-demand application deployment, logon and logoff scripts, and security settings.
- **Simplified service configuration:** Administrators benefit from the integrated setup and configuration features of Windows NT Server 5.0 that are based on Active Directory. These include network services,

application services, and Internet/Intranet services.

- **Improved bandwidth allocation:** The integration of Windows NT Server 5.0 networking services with the Active Directory helps companies improve the cost-effective use of their network by enabling more efficient allocation of network resources to people and applications. Windows NT Server 5.0 networking services such as Reservation Services Virtual Protocol (RSVP)[1] and Quality of Service (QoS)[2] use user profile information in the Active Directory to define the bandwidth, path, and type of services that should be assigned to various users.
- **Security service integration**: Integration of standards-based authentication protocols (e.g., MIT Kerberos and x.509) within the Active Directory enables users to have single sign-on features that span across various networks and applications. Administrators benefit from simpler management of a single set of user accounts that can be enabled to use multiple security credentials including Kerberos or Public Key digital certificates. Administrators can also securely support value chain integration and Extranet scenarios involving partners through the use of digital certificates and mapping of certificates to Windows NT accounts. Application developers can use the security services provided by Active Directory and Windows NT Server 5.0 system to reduce application development cost and complexity.
- **Directory-enabled applications:** Applications written to use Active Directory services offer a number of important benefits. For example, applications can locate service providers dynamically in the directory enabling administrators to reconfigure resources (e.g. specifying on what machines applications should run) as business needs change. Applications can use the directory to locate alternative service providers automatically when preferred providers fail – yielding higher resiliency and application availability to end-users. Active Directory also helps to reduce development time by making it easier for applications locate services already provided by other applications (and published in the directory).
- **Simplified application configuration:** Applications can use the Active Directory and Windows NT Server 5.0 operating system services to centrally store application configuration and installation information. If a user accidentally deletes a configuration file to their application, Active Directory can provide preconfigured installation information back to the application to simplify reinstallation.

Without this level of integration between Windows NT Server 5.0 and the Active Directory, many of these unique benefits would not be possible.

[1] RSVP guarantees the availability of network services along a specific path
[2] QoS guarantees bandwidth for network services

Active Directory's Support for Standards

Because the Active Directory is built from the ground up using Internet standard technologies, customers get the best of proven technologies such as DNS, TCP/IP, LDAP, X.509 and Kerberos that have already been implemented worldwide within organizations and on the Internet. By supporting these industry-standard directory service protocols and interfaces, Microsoft enables user benefits such as single sign-on, centralized management, and network interoperability.

The Active Directory supports the following major standards:

Standards in Windows NT Server 5.0	RFC	Purpose
DHCP	2131	Network address management
Dynamic DNS	2052, 2136	Host namespace management
Simple Network Time Protocol	1769	Distributed Time Service
LDAP v3	2251	Directory access
LDAP 'C'	1777	Directory API
LDIF Directory Information Format	Draft	Directory synchronization
MIT v5 Kerberos x.509 v3 Public Key	1510 ISO	Authentication
~~x.500,~~ LDAP	2247, 2252, 2256	Directory schema
TCP/IP	793 791	Network transport

The benefits of supporting these Internet standards include:

- **Dynamic DNS** enables corporations to achieve a global naming structure that is compatible with standard Internet Domain Naming Standard (DNS) conventions.
- **LDAP** maximizes interoperability between applications and directory services and facilitates directory interoperability through synchronization.
- **Kerberos and X.509 Public Key** Security integration with Active Directory gives corporations the flexibility to mix and match the security they deploy – in both Internet and Intranet environments – based on their needs.

By using standards, customers benefit from full interoperability without

having to change software on existing desktops or servers. However, standards alone are not enough. Vendors must provide complete solutions that integrate with complementary standards. For example, the Active Directory integrates the use of 'RFC822-friendly' Internet names for identifying users in the directory (LDAP), principals in security protocols (Kerberos), certificates (X.509), and in the operating system to dramatically simplify the environment for ends users, distributed applications and enterprise administrators. The result is that customer can integrate Windows NT Server with their existing environment with a minimum of work.

Active Directory Interoperability, Synchronization and Migration

As mentioned earlier, the transition to a global directory will not occur quickly for most companies. There is simply too much directory-related information in too many places. Given that continued proliferation of directory information is so costly in the long-run, however, companies need a strategy for slowing (and eventually stopping) proliferation and moving towards their eventual goal. To that end, Microsoft designed Active Directory to facilitate and expedite the move to a global directory strategy by:

- Supporting interoperability with existing applications via protocols such as LDAP and interfaces such as ADSI
- Providing tools that simplify migration to Active Directory
- Including support for synchronization of data between Active Directory and other directories

Directory synchronization capabilities are important because they enable companies to focus on using Active Directory as their focal point for information storage and management and then propagate subsets of information out to other directories automatically. Synchronization is a key requirement for delivering benefits such as centralized management and single sign-on as companies are in a transition phase with multiple directories to maintain.

Synchronization capabilities will come in several forms. From a standards-based perspective, Microsoft is working with other vendors to ensure that upcoming versions of the LDAP specification will include support for synchronization features – and Microsoft will move quickly to support LDAP synchronization when available. In the shorter term, Microsoft is delivering a one-way synchronization service with Active Directory in the form of 'synchronization connectors'. Active Directory synchronization connectors 'push' changes from the Active Directory into other directories such as NetWare Directory Service (NDS), Netscape Enterprise Directory, Lotus Notes and others. Microsoft will deliver an NDS synchronization connector with the release of Windows NT Server 5.0. Microsoft also expects third parties to deliver synchronization

connectors, using interfaces such as ADSI, to support a number of other directories in the Windows NT Server 5.0 release timeframe.

In the area of migration, Microsoft is working with ~~Cheyenne Software~~Computer Associates to build a migration tool called **DS Migrate for Windows NT**. DS Migrate will enable companies to migrate their NetWare 3.x and 4.x-based servers to Active Directory in an automated fashion. Using ADSI, DS Migrate will copy information from the NetWare Bindery and NDS to a migration engine where it is stored and then mapped automatically to the Active Directory. One advantage of this architecture is that DS Migrate can work online or offline. Companies can either perform an in-place upgrade of their directory information online, or accomplish their migration in several stages offline.

The goal of a single, global directory service is not new. Most companies have used some form of directory service product and have attempted some level of directory integration and standardization. That said, very few companies claim to be as far along as they would like. Inhibiting progress has been products and technologies that excel in one area and fail in others, or require wholesale conversion with no option for preserving existing investments.

Microsoft recognizes this challenge and is delivering both a powerful, enterprise-class technology in the form of Active Directory and a strategy that enables companies to approach the move to a global directory incrementally and pragmatically. Microsoft is also making sure that companies that have made (and will make) investments in Windows NT Server 4.0 have a clear and seamless path to using Active Directory when they choose to move up to Windows NT Server 5.0.

In addition, tight integration of the Active Directory with the Windows NT Server 5.0 operating system will offer greater simplicity, system integrity and powerful new functionality. Clearly, Windows NT Server 5.0 Active Directory provides a standards-based platform for building the next generation of distributed applications and centralized management of the entire network infrastructure.